The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices

J M Blythe*, S D Johnson*

**UCL Dawes Centre for Future Crimes, Jill Dando Institute of Security and Crime Science, UCL, London, UK*
j.blythe@ucl.ac.uk

Keywords: Internet of Things; Cybersecurity; Cybercrime; Consumer security index; Co-design

Abstract

Consumer IoT devices often lack adequate in-built security, giving rise to newer forms of threats and crime risks. Security should be designed into devices but at present there is little incentive for manufacturers to do so consistently. Additionally, consumers are not given simple information at the point of purchase, in user manuals or other materials to help them assess the security of devices. Consumers are therefore not afforded the opportunity to understand the level of security devices offer. Consumer rating indices (e.g. food traffic light labels) can provide this opportunity to aid consumer choice.

This research aims to co-develop a consumer security index (CSI), with consumers and security experts, to aid consumer decision making and incentivise greater security provision in the manufacture of IoT devices. In this paper, we focus on the methodology for the development of the index.

Through a focus group with IoT security experts, Study 1 will identify security features that consumer IoT devices should provide. Study 2 will employ an online survey to identify consumer preferences concerning the disclosure of security and privacy features that devices provide, and focus groups will help to co-design the CSI by discussing the information value, appeal and likely engagement of a security index label. To better understand the current situation, Study 3 will develop a matrix of different classes of IoT devices manually coded according to the CSI for a sample of devices. Study 4 will explore the use of natural language processing to extract data from device user manuals to identify what information is communicated about the security features, as well as, what crime prevention messaging is provided by manufacturers.

The project will use a formal methodology to develop a CSI that is co-designed with experts and consumers. The ultimate aims are to encourage the use of the index to help inform consumer choice, and to lever market action so that IoT devices are shipped with security features in-built.

1 Introduction

The Internet of Things (IoT) brings increasing physical-cyber convergence by providing everyday devices with internet connectivity. For consumers, these devices afford greater convenience, physical security and safety but also bring new and unanticipated crime risks associated with their use. For example, consumer IoT devices have been exploited to disrupt access to popular websites such as Netflix and Twitter [1], children's toys shown to be able to record conversations [2] and baby monitors able to record daily routines and activities [3]. These exploits have largely arisen due to a lack of adequate security built into consumer IoT devices [4].

A lack of security is driven in part by manufacturers desire to be first to market and a lack of incentive to secure devices [5]. This has resulted in manufacturers neglecting thorough and extensive testing of devices before they are sold to consumers. As a result, the burden for protecting devices is often left to the consumer, who may have little or no knowledge of how to do this. Since it is the manufacturers who have the most competency to act, to secure the Internet of Things, devices need to be *secure by design* and have security features built in. One route to incentivising greater security provision is through a label provided at the point of purchase. This would enable consumers to make informed choices, and make explicit what manufacturers should aspire to. As such, there have been calls for a security trust label [6], [7] or a security rating scheme for consumer IoT devices [8], [9].

In the 1980s, few vehicles had integrated immobilisers, or even central locking systems. Despite pressure to do so, manufacturers had little incentive to address this. This changed when the consumer association Which? campaigned to highlight the issues to consumers and the Home Office published the car theft index [10]. These activities acted as a lever to encourage industry to manufacture vehicles with security features as standard, or risk reputational damage. The aim of these four studies is to pursue this in the case of consumer IoT devices through the generation of a simple consumer security index. Our intention would be to co-design the index with industry experts, consumers, retailers and government to develop a consumer rating index that can be easily understood and to develop simple guidance they can follow to reduce their susceptibility to IoT security threats.

Alongside security, consumer privacy concerns inhibit the adoption of IoT devices [11]. IoT devices generate (and share) lots of data about consumers that directly and indirectly reveal their activities and habits [12]. Companies profit from such information through targeted advertising and selling information to third parties. However, companies are often not transparent about the type of information they collect and how it is used. When they are transparent, this is often obscured by burying the details in terms and conditions or a privacy policy, which consumers are unlikely to read. Consumers want more information about, and control over the data about them that organisations collect, use and share [13]. Research has shown that a lack of transparency impacts on consumer trust and that consumers would trust companies more if they were transparent about their data collection practices [14]. We seek to address what and how privacy-related information or features should be communicated to consumers.

Currently, there is no accessible way for consumers to understand the security of a device. This contrasts with the energy efficiency of electronic devices, which in the UK are labelled from A to F to indicate their energy consumption. Presently, if consumers want to protect their internet connected devices, they are required to research the security of the device before purchasing [15]. This would need significant behaviour change by enhancing consumers' capability (to research and understand security concepts and features) and motivation (to prioritise researching security above the functionality, aesthetics, and price of a device) [16]. A security index helps reduce this burden through informing consumers by providing easy to understand information at point of sale. A label allows consumers to choose a device that meets their privacy and security needs. Manufacturers, on the other hand, can use the label to provide this information to their consumers and to differentiate themselves from competing brands, whilst also championing best practice in the security of consumer IoT. Furthermore, a label may also be beneficial in evaluating cyber insurance claims [17] by providing a visual means to assess associated risks of IoT devices.

As governments adopt approaches to encourage self-regulation in markets, the provision of labels at point of sale appears to be an increasingly popular tool, with traffic light systems being used for nutritional content in food and for energy efficiency in electronic goods. The intent of these labels is to simultaneously improve the devices *and* to aid consumer choice. Research suggests that the efficacy and uptake of labels is dependent on the degree to which they are implemented and accessible to consumers. For example, compared to energy labels that use numeric scales, those that use alphabetic ones lead to more consumers buying energy efficient devices [18]. It is important that a security label that is designed to aid consumer choice has value, appeal and can be understood by the target population. Co-designing the label with consumers is intended to ensure it influences their behaviour.

In addition to providing adequate security features (e.g. strong password protection), user compliance is important too. If the use of security features is optional or requires user intervention, users can elect not to employ them, or can do so half-heartedly (e.g. using weak passwords), compromising the effectiveness of any measures in place. Users may not employ particular security features because they are simply not aware that such features exist, the implementation of the security features does not follow usable security best practice, or because they do not know how to configure them. Alternatively, they may understand what the features are, but purposefully decide not to use them (e.g. using an existing password rather than creating a new one). User compliance, and improving this (e.g. not allowing the device to function where default passwords are used) is consequently perhaps as important as the security features themselves. However, manufacturers may not adequately explain the importance of the security features in user manuals. There is a lack of research around how manufacturers communicate to users about features in manuals and the types of crime prevention messaging they may adopt to influence consumer behaviour change. Consequently, we seek to address how security features and crime prevention advice is explained to consumers in device manuals.

For the CSI to influence the market and consumer choice, a number of issues will need to be addressed. First, unlike existing labelling schemes, such as those for energy efficiency, the resilience of a device to attack changes over time as vulnerabilities are discovered and new hacking methods developed. Second, there are challenges with objectively measuring security as the IoT is complex and involves multiple components such as hardware, apps and the cloud [19]. Third, unlike food labelling and energy efficiency, there is an adversary in the cybersecurity context. Thus, a potential unintended consequence of an incorrectly implemented label is that it would provide offenders with specific information on device vulnerabilities that they could exploit. Hence, it is equally important that the label does not provide further routes for exploitation. Next, we outline previous approaches to security rating scales and how they address such issues.

Loi et al. (2017) recently developed a rating index which involves security tests to assess four dimensions of security: (i) confidentiality of data, (ii) integrity and authentication of device connections, (iii) control and availability of device to connection requests, and (iv) capability of device to participate in attacks. They assessed 20 consumer IoT devices on the four dimensions to provide a three tier rating scale from "secure", "moderately secure" to "insecure". They found that all devices tested had shortcomings in one of the four dimensions, highlighting issues in the security of consumer IoT. They did not address the issue of the security posture of a device changing over time but do provide an objective way of measuring the security of IoT devices. However, this approach requires significant testing which could significantly increase the price of cheaper classes of IoT devices and be a barrier to market entry for start-ups and small businesses.

Others have suggested alternatives to the explicit testing of IoT devices in the deviceion a rating system. Jamieson (2016) argues that a rating system can be based on the "vulnerability surface" of a device. Jamieson defines this as the interfaces,

processing attack surface, and system architecture of a device. Devices with more interfaces and a greater attack surface are considered less objectively secure, whereas the specific system architecture can either help or hinder the device security. Jamieson outlines the Logical Security Posture (LSP) as a metric to measure this in which points are assigned for the presence of security features and points deducted for features that increase the attack surface. They argue that such a rating system represents the device's resistance to attack and that a device's security is dependent upon a manufacturer's commitment to providing updates, with stars lost for not doing so. They also consider the issue of the longevity of "security" by explicitly stating the years for which the rating applies. Finally, they suggest a follow up service for on-site inspections which can remove stars if the design of the device has been surreptitiously changed.

The CSI seeks to build on this initial work by Jamieson (2016) and provides some further advantages over these existing approaches. Firstly, it will be systematically designed with experts and users and co-ordinated with industry and government rather than a single entity. Integrating consumers in to the design process helps ensure that the label will influence consumer choice and manufacturer aspirations as intended. The CSI will also go beyond labelling as it focuses on heightening consumer awareness through manuals and addressing crime prevention messaging to influence behaviour change in consumers.

In this paper, we detail a protocol which outline a methodology for developing the security index. Protocols are increasingly used in science, particularly disciplines such as medicine and health psychology. They help improve the standard of research [20] by (i) allowing researchers to obtain feedback on study designs through peer review, (ii) enabling readers to compare what was originally intended with what was actually done in future publications, which prevents p-hacking and post-hoc revision of study aims, and (iii) enabling researchers, funders and policy makers to see what studies are underway and reduce potential research duplication. The work outlined here is being conducted in parallel to a systematic review of crimes that can be facilitated by consumer IoT devices.

1.1 Overall Aims

To co-develop a consumer security index (CSI), with consumers and security experts, to aid consumer decision making and incentivise greater security provision in the manufacture of consumer IoT devices. In the sections that follow, we outline the aims of each study in more detail and discuss the methodology to be adopted in each case.

2 Study 1: Security and privacy features of consumer IoT devices

2.1 Aim

The aim of Study 1 is to identify security and privacy features of consumer IoT devices by using expert consensus methods to elicit and encapsulate current thinking.

2.2 Methods

2.2.1 Participants

Participants will be seven IoT security experts with extensive experience in the security of IoT consumer devices.

The experts will be recruited via email from those who have previously participated or are associated with the PETRAS Internet of Things Research Hub, from an expert advisory panel assembled for the Secure by Design policy review conducted by the Department for Digital, Culture, Media, and Sport (DCMS), and from scientific and professional societies and centres (Dawes Centre for Future Crime at UCL, Research Institute in the Science of Cybersecurity) and from government departments (National Cyber Security Centre, Home Office and the DCMS). We will also use snowball sampling by asking for recommendations from those already recruited. We will seek to a gain balance of experts from academia, government, retail, and industry.

To ensure the suitability of the sample, potential participants will be asked to complete a self-assessment questionnaire to evaluate their relevant expertise in IoT security. Questionnaires assessing expertise have been shown to be a predictor of initial accuracy of judgement in expert consensus exercises [21]. Participants will be included if they rate their expertise in IoT security as ≥ 5 (on a 7-point scale, where 0 indicates 'no expertise' and 7 indicates 'profound expertise'). We will also corroborate their expertise through web searches.

2.2.2 Procedure

2.2.2.1 Consensus Development Method

The Nominal Group Technique (NGT) will be used for formal consensus development [22]. NGT allows feasible and reliable facilitation of face-to-face group discussion through explicit and replicable steps to reach consensus on a topic of discussion [23]. Compared to conventional focus groups which aim to discuss an issue in-depth, consensus methods such as NGT also allow for prioritisation or agreement on solutions [23]. The structured format of NGT also prevents the domination of a single participant and encourages all members to participate in discussions [24].

We will run a focus group with the experts and follow the four key stages of NGT:

1. **Silent generation** – Prior to the workshop, participants will be sent a series of questions regarding key security and privacy features for

consumer IoT and also allowed up to 20 minutes in the workshop to reflect on their responses [25]. These features will be based on the DCMS's Secure by Design Code of Practice for Consumer IoT and other related guidance and principles.

2. **Recording ideas** – During this stage, participants will be asked (one at a time) to provide a single idea to the group in a "round robin" fashion. Each response will be recorded and no debate allowed. New ideas will be welcomed but participants will be required to wait their turn. The process will continue until no new ideas are generated.
3. **Clarification** – At this stage, participants may propose the exclusion, inclusion or modification of ideas [26]. They may also discuss the clarity and importance of each item [24]. With group agreement, ideas will be clustered and all ideas discussed to ensure participant understanding [27].
4. **Voting** – Participants will privately vote on their top preferences from the generated ideas. Votes will then be tallied to identify ideas that are rated highly.

2.2.3 Data Analysis

Participants' responses will be presented in a ranked tally table, with security features that have a greater percentage agreement considered to be most important for the index. The following questions will be addressed through the analysis:

1. What proportion of experts rate certain features higher than others?
2. What features are ranked most and least highly?

3 Study 2: Consumer preferences for the CSI

3.1 Aim

The aims of Study 2 are to i) identify consumer preferences concerning the disclosure of security and privacy features that devices provide (Study 2a) and ii) co-design the label by discussing the information value, appeal and likely engagement with a security index label (Study 2 a/b).

3.2 Study 2a

To gain insight into consumers' preferences, we will conduct an online study in which participants will be asked to rank security and privacy-related features that they would like to be communicated to them.

3.3 Methods

3.3.1 Participants

Participants will be eligible to take part if they i) are aged ≥ 18 years and ii) live in the UK. We will aim to gain a quota sample of 1000 participants representative of the UK population in terms of age and sex and will recruit participants through the online panel company "prolific.ac".

3.3.2 Design

The study will use a between-subjects design with groups asked about different types of consumer IoT device. Participants will be asked about specific devices (as opposed to an unspecified device) to ensure that they use the same frame of reference when answering questions. This is to avoid any confounding effects that might otherwise arise. The independent variable will be the type of IoT device (Wi-Fi Router, Smart TV, Smart Thermostat, Smart Watch and Smart Security Camera) selected from the most popular sold consumer IoT devices on Amazon. The dependent variable will be the ranking of importance of security and privacy-related information.

3.3.3 Stimuli

Participants will be asked to rank order approximately 17 items covering both security and privacy-related information that they would like to be communicated to them. An example security-related item is "*The device's support period (how long the device will receive security updates until it is no longer supported)*" and an example privacy-related item is "*Whether my personal data is shared with third party companies"*. The items will be developed based on previous research on labelling schemes (e.g. [28]) and through discussion with academics and industry.

3.3.4 Procedure

Participants will first be provided with information about the study and asked to provide consent to take part. They will then be allocated to one of five device conditions. Next, they will be provided with information about existing labelling schemes they may be familiar with (e.g. the traffic light system used for food devices and energy efficiency labels). They will then be informed that we are interested in developing a similar label for internet connected devices based on what is important to consumers. Participants will be asked to rank what information they would like the label to communicate to them before purchase for the device they were allocated to consider and provided with a short description of each feature alongside each item.

3.3.5 Data Analysis

The following questions will be addressed:

1. Do participant rankings significantly differ by type of IoT device?
2. What features are ranked most and least highly by consumers?

3.4 Study 2b

To gain further insight into consumers' preferences and to co-design the label, in Study 2b we will conduct a workshop with consumers.

3.4.1 Participants

Participants will be eligible to take part if they i) are aged ≥ 18 years and ii) live in the UK. We will obtain an opportunity sample of participants who live in London and surrounding areas, recruited via UCL and through the user partners of the

PETRAS Internet of Things Research Hub. Seven participants will be recruited per focus group. Will run 2-3 focus groups until saturation is reached [29].

3.4.2 Design and procedure

The workshop will last approximately 2 hours and will be facilitated by the lead author.

The workshop will cover the following topic areas:

- The role and value of a security label and their likely engagement
- Preferences around security and privacy features
- The appeal of different concepts of label designs

Following introductions, participants will be asked to discuss their opinions and concerns around the security and privacy of consumer IoT devices (15 mins) as a warm up activity. They will then discuss the role of a security label and their likely engagement (25 mins). Subsequently, participants will discuss the key security and privacy features as identified in Study 2a (40 mins). As a final activity (40 mins), participants will be shown the label concepts one by one and asked to score them individually on a 1–10 scale and write down their likes and dislikes for each one. They will then discuss each concept as a group and be probed further to express their thoughts and understanding of the labels. At the end of the session, respondents will be asked to share any final thoughts.

3.5 Data Analysis

The following questions will be addressed:

- What are participants' thoughts on the role and value of a security label and their likely engagement?
- What features are considered most and least important by consumers?
- Which label design concepts are most preferred by participants and why?

4 Study 3: IoT devices coded to the CSI

4.1 Aim

The aim of Study 3 is to develop a matrix of different classes of IoT devices manually coded according to the CSI for a sample of devices.

4.2 Method

We will obtain a representative sample of 40 open source user manuals for different classes of consumer IoT devices sold by high-street retailers and systematically code them to extract information on the security features they provide.

A coding scheme will be developed based on the findings from study 1 and study 2. We will also discuss and refine the coding scheme with the expert panel assembled for Study 1. This will ensure that the coding scheme is fit for purpose and that we have not missed any important details.

We will use framework analysis [30] to code for the presence or absence of security and privacy features according to the coding scheme. Framework analysis allows the coding scheme to be further refined through themes that may emerge through the qualitative analysis of the user manuals that were unaccounted for in the initial coding scheme.

To ensure inter-rater reliability, during a pilot exercise prior to the main activity, two raters will be trained to use the coding strategy, and they will independently code a sample of user manuals. Their ratings will subsequently be compared using indices of inter-rater reliability (e.g. Cohen's Kappa) and the coding strategy updated, or further training provided, as necessary. Coder drift, which can occur when a coder changes how they apply the coding criteria over time, will also be monitored throughout the coding exercise.

4.3 Data Analysis

The following questions will be addressed:

- What security and privacy features are currently offered by consumer IoT devices?
- How does the presence or absence of these features differ across classes of consumer IoT devices?

5 Study 4: How do manufacturers communicate information?

5.1 Aim

The aim of Study 4 will be to extract data from device user manuals to identify what information is communicated to users about the security features devices offer and what crime prevention messaging is provided by manufacturers.

5.2 Method

We will obtain a representative sample of 40 open source user manuals for different classes of consumer IoT devices sold by high-street retailers and systematically code them to extract information about what information is communicated by security features and what crime prevention messaging is presented in manuals.

A coding scheme will be developed by two researchers based upon on an analysis of a sub-set of the manuals and will be coded qualitatively using framework analysis [30]. We will also explore the extent to which this can be automated using natural language processing.

5.3 Data Analysis

- What information relating to security and privacy features is communicated to consumers by manufacturers?
- What crime preventing messaging is communicated to consumers by manufacturers?

6 Discussion

A consumer security index has the potential to influence manufacturers to provide greater security provision in consumer IoT and also influence consumers to purchase more secure devices. Currently, devices are not shipped with

adequate security built in and there is no accessible way for consumers to understand the likely security afforded by a device before buying it (or even after buying it). Previous studies that have discussed security labels for IoT devices have not been systematically developed and co-designed with consumers or those who might promote them such as government policy leads and retailers. By doing so we hope to maximise the utility of the label. The series of studies discussed above have a number of additional strengths. First, by collecting and evaluating data from experts and consumers, it will contribute valuable information about how these different groups consider the importance and content of the label. Secondly, this will be the first label that is systematically developed with industry, retailers, consumers and government. Third, the inclusion of an analysis of how information is communicated in manuals about crime prevention messaging provides valuable information about how security features are currently explained to consumers and how manufacturers might encourage protective behaviour.

6.1 Limitations

A limitation of the studies is the reliance on consumers' hypothetical engagement with the label. This may limit the applicability of the findings to actual uptake of the label in the wild. The studies outlined here represent the initial development of the CSI but future experimental work will be required to objectively assess the effectiveness of different design concepts on consumer purchasing behaviour.

6.2 Dissemination and Implementation

We will increase awareness of the Consumer Security Index through dissemination of the work and implementation of the findings.

We will promote the CSI to maximise its potential to influence market forces. To achieve this, we will engage in the following dissemination activities. The findings from this study will first be disseminated to the PETRAS Internet of Things Research Hub, government departments (DCMS, Home Office and National Cyber Security Centre) and industry partners. Second, we will disseminate to the public and wider community through IoTUK. Finally, we will disseminate to academic researchers and policymakers via academic conference presentations and journal articles.

6.3 Ethics

The research outlined in this protocol paper will be approved by the University College London Research Ethics Committee. All procedures performed in the studies involving human participants will be conducted in accordance with the ethical standards of this committee and with the 1964 Declaration of Helsinki and its later amendments. Informed consent will be obtained from all individual participants.

7 Acknowledgements

"This work was funded by the UK EPSRC as part of the PETRAS IoT Research Hub - Cybersecurity of the Internet of Things grant no EP/N02334X/1, and the Dawes Centre for Future Crime."

8 References

[1] BBC news, "Mirai botnet: Three admit creating and running attack tool," 2017. [Online]. Available: http://www.bbc.co.uk/news/technology-42342221.

[2] Which?, "Safety alert: see how easy it is for almost anyone to hack your child's connected toys," 2017. [Online]. Available: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/.

[3] NYC Consumer Affairs, "Consumer Alert: Consumer Affairs Warns Parents to Secure Video Baby Monitors," 2016. [Online]. Available: https://www1.nyc.gov/site/dca/media/pr012716.page.

[4] B. Schneier, "Click Here to Kill Everyone," 2017. [Online]. Available: http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html.

[5] M. Sadler, "Securing our connected world," 2017. [Online]. Available: https://dcmsblog.uk/2017/10/securing-connected-world/.

[6] Microsoft, "Cybersecurity policy for the Internet of Things," 2017.

[7] Infineon et al, "Common position on cybersecurity (Infineon - NXP - STMicroelectronics - ENISA)," 2016.

[8] The Guardian, "Smart fridges and TVs should carry security rating, police chief says," 2017. [Online]. Available: https://www.theguardian.com/technology/2017/jul/24/smart-tvs-fridges-should-carry-security-rating-police-chief-says.

[9] A. Jamieson, "IoT Security - It's in the Stars!," 2016. [Online]. Available: https://www.slideshare.net/AndrewRJamieson/iot-security-its-in-the-stars-169-v201605241355.

[10] G. Laycock, "The UK car theft index: An example of government leverage," in *Understanding and preventing car theft, vol. 17 of crime prevention studies*, 2004, pp. 25–44.

[11] Businessinsider, "Consumers are holding off on buying smart-home gadgets thanks to security and privacy fears," 2017. [Online]. Available: http://uk.businessinsider.com/consumers-holding-off-on-smart-home-gadgets-thanks-to-privacy-fears-2017-11.

[12] FTC, "IoT Privacy & Security in a Connected World," 2015.

[13] J. Phelps, G. Nowak, and E. Ferrell, "Privacy Concerns and Consumer Willingness to Provide Personal Information," *J. Public Policy Mark.*, vol. 19, no. 1, pp. 27–41, Mar. 2000.

[14] K. L. Walker, "Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection,"

J. Public Policy Mark., vol. 35, no. 1, pp. 144–158, 2016.

[15] J. M. Blythe, S. Michie, J. Watson, and C. E. Lefevre, "Internet of Things in Healthcare: Identifying key malicious threats, end-user protective and problematic behaviours," in *Frontiers in Public Health*, no. 21.

[16] S. Michie, M. M. van Stralen, and R. West, "The behaviour change wheel: A new method for characterising and designing behaviour change interventions," *Implement. Sci.*, vol. 6, no. 1, p. 42, 2011.

[17] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically Evaluating Security and Privacy for Consumer IoT Devices," *Proc. 2017 Work. Internet Things Secur. Priv. - IoTS&P '17*, pp. 1–6, 2017.

[18] London Economics, "Study on the impact of the energy label and potential changes to it – on consumer understanding and on purchase decisions," 2014.

[19] Alliance for Internet of Things Innovation, "AIOTI Digitisation of Industry Policy," 2016.

[20] Biomed Central, "Publish your study protocol," 2017. [Online]. Available: https://old.biomedcentral.com/authors/protocols.

[21] G. Rowe and G. Wright, "The impact of task characteristics on the performance of structured group forecasting techniques," *Int. J. Forecast.*, vol. 12, no. 1, pp. 73–89, 1996.

[22] A. H. Van de Ven and A. L. Delbecq, "The nominal group as a research instrument for exploratory health studies.," *Am. J. Public Health*, vol. 62, no. 3, pp. 337–342, Mar. 1972.

[23] S. S. McMillan, M. King, and M. P. Tully, "How to use the nominal group and Delphi techniques," *Int. J. Clin. Pharm.*, Feb. 2016.

[24] Center for Disease Prevention, "Gaining consensus among stakeholders through the nominal group technique," 2006.

[25] D. J. Claxton, R. B. J. Ritchie, and J. Zichkowsky, "The nominal group technique: It's potential for consumer research," *J. Consum. Res.*, vol. 7, no. 3, pp. 308–313, 1980.

[26] P. Bissell, P. Ward, and P. Noyce, "Appropriateness measurement : application to advice-giving in community pharmacies," *Soc. Sci. Med.*, vol. 51, no. 3, pp. 343–359, 2000.

[27] A. L. Delbecq, A. H. Van de Ven, and D. H. Gustafson, *Group techniques for program planning: A guide to nominal group and Delphi processes*. Scott Foresman, 1975.

[28] P. Kelley, J. Bresee, L. Cranor, and R. Reeder, "A nutrition label for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009.

[29] G. Guest, E. Namey, and K. McKenna, "How many focus groups are enough? Building an evidence base for nonprobability sample sizes," *Field methods*, pp. 1–20, 2016.

[30] J. Ritchie and L. Spencer, "Qualitative data analysis for applied policy research," in *Analyzing qualitative data*, Abingdon, UK: Taylor & Francis, 2002, pp. 173–194.